LA UNIVERSIDAD Y SU RELACIÓN CON LA CIBERSEGURIDAD

Carlos Hernández Rodríguez[*], Milagros Cano Flores[&], Teresa García López[&]

INTRODUCCIÓN

Actualmente nuestro País enfrenta altos índices de inseguridad, lo cual origina a la sociedad mexicana una gran preocupación, pero se ha añadido a ese gran problema un motivo más para sentirnos inseguros, y es a través el uso del internet y redes sociales.

Debido a esta situación el Sistema Nacional de Seguridad Pública, a través de sus instancias competentes e instituciones de colaboración, se esfuerza por dar solución a los actos ilícitos que perturban la paz y tranquilidad social.

Cabe destacar, que el Sistema Nacional de Seguridad Pública es la encargada de planear y aplicar acciones que conlleven a una seguridad social, pero también es preciso resaltar que todos los ciudadanos como miembros activos de la sociedad también debemos contribuir al logro de las mismas. Sin embargo, hoy en día no solo estamos expuestos a un asalto, robo entre otro ilícito,

[*] Doctor en Administración y en Educación
[&] Doctora e Investigadora del Instituto de Investigaciones y Estudios Superiores de las Ciencias Administrativas
[&] Doctora e Investigadora del Instituto de Investigaciones y Estudios Superiores de las Ciencias Administrativas

si no que estamos expuesto al robo de datos que almacenamos en dispositivos que ahora son vulnerables.

Las instancias que se encuentran dentro del Sistema Nacional de Seguridad Pública, no deben ser las únicas promotoras de la seguridad, las universidades a través de su primordial función de formación académica, investigación y difusión en diferentes áreas del conocimiento pueden contribuir de manera significativa en la búsqueda de soluciones, en relación a la gestión de soluciones que conlleven a evitar ilícitos a través del uso de los desarrollos tecnológicos.

Prácticamente nada escapa a la digitalización y las personas, las empresas y las instituciones se ven abocadas a vivir y funcionar cada vez más en la red. Obviamente esto constituye un escenario de oportunidades de todo tipo, pero, también trae consigo nuevas amenazas relacionadas con la vulnerabilidad del usuario de la red.

El objetivo esencial de este trabajo consiste en mencionar la importancia de establecer un vínculo Universidad-Sociedad, para que en conjunto se elaboraren proyectos estratégicos que conlleven a entender y mejorar la Ciberseguridad.

¿QUÉ ES LA CIBERSEGURIDAD?

La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el

ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. [Unión Internacional de Telecomunicaciones (UTI), 2010).

El número y el grado de sofisticación de los ciberataques están aumentando al mismo tiempo que crece nuestra dependencia de Internet y de otras redes para obtener servicios e información críticos. De acuerdo con la compañía de seguridad McAfee, en 2011 se produjo el mayor número de amenazas descubiertas. Se supone que existen aproximadamente unos 70 millones de programas malware circulando en todo el mundo y los teléfonos inteligentes ("smartphones") se han convertido en el principal medio de su difusión. Los analistas consideran que al menos el 70% de los correos electrónicos son spam. Mientras tanto, las redes eléctricas inteligentes, la computación en nube, las redes de automatización industrial, los sistemas de transporte inteligentes, la ciberadministración y la banca electrónica, entre otros tipos de infraestructura, se están interconectando. (UTI, 2012)

Sin embargo, la mayor facilidad de conexión y la mayor eficacia en las comunicaciones traen consigo una mayor vulnerabilidad frente a los ciberataques. Aún no existe una definición de ciberseguridad aceptada en todo el mundo y ello obstaculiza los esfuerzos de protección que deben emprenderse a nivel nacional e internacional teniendo presente el carácter transfronterizo que tienen hoy en día las redes y sistemas informáticos. Para el año 2015 más del 60% de la Población mundial hace uso del internet, esto ha aumento significativamente los ataques cibernéticos, el robo de información, de identidad, entre otros.

El problema es que aunque el usuario presenta preocupación por su ciberseguridad, a menudo no es capaz de identificar cuáles son realmente los peligros y por tanto no sabe cómo enfrentarse

a ellos. Por ejemplo, gran parte de los internautas piensa que la mayor amenaza en la red es que te roben datos personales y las claves, pero el cibercrimen evoluciona constantemente, de forma que un atacante puede querer acceder a los recursos del usuario para aprovecharse del poder de procesamiento con el fin de realizar tareas que requieran gran poder de computación, o bien puede robarle su ancho de banda para que su sistema actúe como un zombi dentro de una *botnet* y poder realizar ataques masivos. (Rodríguez, 2016)

Por otro lado, el **Cloud Computing** se ha convertido en poco tiempo en una importante tendencia tecnológica, pero entraña numerosos riesgos relacionados con la seguridad, como la pérdida de control en el uso de las infraestructuras de la nube, la falta de garantía de la seguridad de los datos y las aplicaciones cuando se lleva a cabo la portabilidad a otro proveedor, los fallos de aislamiento, los problemas a la hora de realizar certificaciones externas de seguridad o calidad de los servicios de la empresa que opera en la nube o la exposición que supone el llevar a cabo la gestión de las interfaces a través de Internet. Por su parte, en el caso del **Big Data**, el almacenamiento y tratamiento de enormes cantidades de datos es en sí un riesgo para la seguridad, puesto que las filtraciones o robos de información pueden tener importantes efectos legales y reputacionales para una organización. (Rodríguez, 2016)

Por otra parte, actualmente las **apps** constituyen el medio preferido para conectarse a la red desde dispositivos móviles. Para valorar su importancia, es importante saber que el 90% del tiempo de conexión a Internet a través de un dispositivo móvil se destina a su uso y cada mes se lanzan al mercado unas 40.000 nuevas apps. La principal ciberamenaza en este caso es la capacidad que tienen de recolectar datos personales y de comportamiento lo que las convierte en un foco de posibles fugas de información que afecten a la privacidad del usuario. A esto hay que sumarle que su carácter global choca con las

distintas legislaciones sobre la protección de la privacidad que existen en los distintos países. (Molano, 2016)

Las soluciones de seguridad pueden pasar por el uso de software específico de privacidad en los teléfonos móviles, pero realmente resulta fundamental informar y concienciar al usuario sobre la adecuada gestión de su privacidad en las redes.

Hasta ahora se han visto una gran cantidad de ataques y tendencias que indican que los ataques M2M están a la alza, por lo que las preocupaciones por la seguridad del Internet de las Cosas están bien fundamentadas. Gartner ha estimado que 6.4 mil millones de nuevos dispositivos para el IoT se incorporarán al Internet durante el 2016. (Manky, 2016)

También podemos ver la posibilidad de que este tipo de ataques se expandan más allá del crimen informático para convertirse en terrorismo o guerra cibernética. De acuerdo con la Base de Datos Nacional sobre Vulnerabilidades (NIST), estamos en camino de ver un número, sin precedente, de CVEs (Vulnerabilidades Comunes y Exposición). La información más reciente de NIST sobre CVE muestra que cerca de 4.200 de vulnerabilidades comunes se han encontrado en software disponible al público, las mismas que ya han sido divulgadas y publicadas, por lo que nuestra predicción es que aún faltan muchas más por ser descubiertas. (Manky, 2016)

Así como los cibercriminales se vuelven objetivo de investigaciones y enjuiciamientos dentro del sistema de justicia criminal, los hackers que son cuidadosos han desarrollado una nueva variante de malware llamado 'ghostware', diseñado para cumplir con su misión y después borrar cualquier huella antes que las medidas de seguridad puedan detectar que el sistema ha sido comprometido.

Este tipo de ataques sobrepasan las técnicas y herramientas de prevención. La detección en tiempo real es esencial, ésta requiere un enfoque de arquitectura de seguridad integrada, que permita que los dispositivos compartan información sobre el ataque, en tiempo real, correlacionen y generen inteligencia de amenazas accionable y coordinen una respuesta para aislar el malware para, de esta manera, poder identificar todas las instancias del ataque desplegado en cualquier lugar de la red. (Manky, 2016)

Se esperan ver más ataques basados en 'Ghostware' que han sido rediseñados para explotar el doble desafío que representan, por un lado, el incremento en la brecha de habilidades de seguridad y, por el otro, los dispositivos aislados de seguridad heredada. (Manky, 2016)

De acuerdo con el estudio 'Market Pulse Suvey', el 69% de las personas que fueron alguna vez empleados pero ya no hacen parte de la nómina de las compañías, todavía tiene acceso a la información corporativa. Así mismo, un 83% de las personas que accede a las nubes corporativas también tiene instalado en sus dispositivos lo que se conoce como 'shadow IT', o tecnología sombra, que puede ayudar a resolver tareas cotidianas pero no cuenta con el aval del área TI.

Las cifras anteriores debieron activar una alarma de seguridad entre todos aquellos que valoran los datos de sus organizaciones, y no es para menos, cuando entre tanta información aquella que servirá para la toma de decisiones que agregarán valor a un negocio. (Molano, 2016)

Por lo tanto la Ciberseguridad es un tema que está cobrando relevancia y trascendencia y aunque para muchas personas, el término no es familiar aún, en poco tiempo quizás estemos

pagando a una empresa especial dedicada a la vigilancia de nuestra información en la red, tal y cual cuidaran nuestra casa.

LAS UNIVERSIDADES COMO GENERADORAS DE CONOCIMIENTO

El término universidad se aplicaba a toda comunidad organizada con cualquier fin, cuando los profesores de las escuelas formaron comunidades para proteger sus intereses, el término "Universidad" comienza a aplicarse por excelencia a las comunidades de profesores y estudiantes, se pasa de la escuela a la universidad como institución autónoma. El proceso de transformación fue gradual y se llevó a cabo de manera diferente para cada universidad. (Tunnermann, 2003)

La institución universitaria, durante su larga vida que se aproxima a los ocho siglos, ha sufrido profundas transformaciones a origen de los distintos movimientos culturales. La sobrevenida más importante a fines del siglo XVIII, fue la secularización de la enseñanza el Estado sustituyó a la iglesia en la alta dirección de la empresa docente. (Tunnermann, 2003)
La problemática actual se encuentra en el debate acerca de los fines de la universidad. En el siglo pasado se manifestó un fuerte contraste entre las instituciones educacionales inglesas y las del continente. Donde las primeras plasmaron el tipo humano, donde se dedicaron a la formación de la personalidad. En el continente, sobre todo en los países latinos, la universidad asumió la misión principal de conservar y transmitir los conocimientos y suministrar a la vez una sólida base para el ejercicio de las profesiones (abogados, médicos, ingenieros, farmacéuticos, entre otros) a cuyo fin expedía los correspondientes títulos.

Ambos ideales, la formación integral humana y la conservación del saber, pertenecen a las finalidades imprescriptibles de la

institución universitaria. Pero esta enfrenta ahora nuevas exigencias como consecuencia de la profunda transformación social a que estamos asistiendo. La mera transmisión del saber no satisface ya; a la universidad se le pide que promueva la obtención de conocimientos nuevos y contribuya al incesante incremento de la ciencia. Al empuje de esta necesidad, junto a las cátedras universitarias y a título de complemento obligado a ellas, se organizan seminarios y laboratorios en los que florece la especulación pura. Por esta razón la función investigadora ha pasado a ser primordial en la universidad de hoy. (Tunnermann, 2003)

Otro problema que ha de resolver la universidad de hoy es el de la fijación de sus fronteras, el progreso científico requiere de una creciente especialización. La vinculación usual entre función docente y la investigadora encauza esta antítesis hacia una solución; a la primera se le reserva la integración de los conocimientos en visión sintética y unitaria, en tanto que la segunda permite ahondar el análisis y la especialización hasta donde sea posible.

Las Universidades son instituciones de educación superior, centros con cierta complejidad organizativa, que integran diversas facultades de artes, ciencias y escuelas profesionales las cuales poseen autoridad para conferir títulos en varios campos del saber. Son organizaciones dedicadas a hacer avanzar el saber, que enseñan e investigan, esto es, generan, enseñan y difunden el saber.

En México, la universidad durante muchos años, se configuraba de acuerdo con el modelo francés, el cual tiene como ideal: (lograr la estabilidad política del Estado; su procedimiento es de una enseñanza profesional uniforme confiada a un cuerpo organizado; su función es crear un motor intelectual a través de una función asignada por la sociedad), sin embargo, el surgimiento de las universidades privadas y la incidencia es

éstas para cubrir la demanda laboral muestran indicios de un cambio radical en el esquema universitario, tanto en sus ideales como en sus procedimientos.

A partir de 1968 hay una búsqueda por la democratización en la que se pretende una mayor participación de los alumnos en las decisiones. Un giro en la conformación del sistema universitario lo ha dado el hecho de que el gobierno va perdiendo papel protagónico en su financiamiento, así como en sus funciones, orientación y control, y va ganando terreno la autonomía en la generación y difusión del conocimiento en el nivel superior dentro de la enseñanza formal.

Los sistemas universitarios actuales tienen una marcada tendencia a la especialización que se acentúa que se acentúa por el gran auge que se le da a la actividad económica y al individualismo, el cual deriva un espíritu utilitarista; sin embargo, por otro lado ¿existe un ansia por saber y entender el todo que rodea al hombre, lo que puede propiciar el mantenimiento de la idea de una formación más generalizada y una enseñanza de carácter holístico a pesar de la tendencia a hacer de las universidades entidades generadoras de profesionistas que surtan la demanda del carácter laboral. (Tunnermann, 2003)

La universidad pública, considerada como una institución eminentemente cultural, tiene como metas la producción y transmisión de formas de saber, y la formación de intelectuales (profesionales e investigadores) con conciencia crítica y posición activa sobre su desempeño social, lo que responde así a los intereses globales de amplios sectores de la nación, y no sólo a los del gobierno o la empresa. (ANUEIS, 2014)

El conocimiento forma parte de la realidad. El conocimiento puede generarse dependiendo del contexto donde esté involucrada un problema en particular. Esa realidad puede ser

entendida dependiendo de la formación del investigador o disciplina desde donde se estudie el problema. En la generación del conocimiento, juega un papel importante el contexto donde esté involucrada la realidad, y de acuerdo a los resultados obtenidos de puede actuar en lo social, lo cultura, lo económico y lo histórico, tratando de obtener un beneficio colectivo.

Por ello la Universidad está obligada a generar conocimiento que permita administrar en forma eficaz la información almacenada en la red, pero también a desarrollar programas que permitan contrarrestar una amenaza cibernética, si bien es cierto que en las universidades se han formado individuos que han provocado el avance de la tecnología, hay otros que han desarrollado su conocimiento de manera informal.

Por lo anterior, la gestión del conocimiento es una toma de conciencia del valor del conocimiento como recurso y producto en la sociedad. El conocimiento es uno de los valores más preciados que pueda tenerse y buscarse. No debemos olvidar que esta búsqueda y hallazgo se dio en primer lugar en las organizaciones empresariales. En ellas se reconoce la necesidad imperante de acelerar flujos de información desde los individuos hacia la organización y vice-versa con la intensión de producir un valor agregado para la organización. La información se convierte a través de los individuos en un activo de conocimiento para la organización y éste, a su vez, en un "activo de capital humano" (Minakato, 2009).

LA UNIVERSIDAD Y SU RELACIÓN CON LA CIBERSEGURIDAD

El primer problema de este tema, es la conceptualización del término seguridad al que se le han intentado agregar campos que no le corresponden. La Seguridad Pública, es la función a cargo del Poder Ejecutivo, mediante la cual, a través de acciones

efectivas de información, disuasión y actuación firme, se logra la prevención de conductas delictivas, garantizando con ello, la tranquilidad e integridad de cada uno de los integrantes de la sociedad. Esta función forma parte de todo un sistema penal, que involucra diversos sectores y a los tres poderes de la Unión, en el afán de combatir el delito y castigar a sus autores. (Aguayo, 1999)

La Seguridad Pública es tan sólo una de las funciones concretas que tiene a su cargo el Ejecutivo para prevenir los delitos, más no la única. Quinientos años antes de Cristo, Confucio escribió lo siguiente: "Cuando se le conduce al pueblo mediante disposiciones y órdenes administrativas, y cuando por medio de castigos se procura meterle en razón, ciertamente que el pueblo evitará los delitos, mas no tomará conciencia de que la comisión de delitos es algo de lo que tiene que avergonzarse. Cuando mediante la fuerza de unos principios morales se le guía exteriormente hacia el bien y se vinculan sus actividades externas a un extenso catálogo de formas de comportamiento ritualizadas, entonces tendrá el sentimiento de vergüenza, se apartará del mal y marchará por el camino correcto". (Aguayo, 1999)

> La Doctrina de la Seguridad Nacional tiene sus orígenes en la necesidad que el gobierno tiene de evitar problemas en la conducción del país. (CNS, 2015)

La educación, es uno de los medios por excelencia para enseñar normas y valores a las personas para alejarlas del delito, es un elemento fundamental para transmitir de manera implícita en los planes curriculares de las instituciones educativas, una cultura de valores que propicie en los sujetos una participación sólida ante su sociedad, en aspectos relativos a la sociedad.

Dentro de la seguridad pública, también ha existido una adaptación a las nuevas formas de delito que se pude cometer en la sociedad, y es a través del uso de recursos tecnológicos, mejor llamados "cibernéticos", por lo tanto, los Gobiernos han tenido que diseñar estrategias para proteger a la sociedad de ilícitos que cada vez más se dificultad en atrapar al delincuente, pues ahora se enfrentan a entes digitales, que pueden provocar un problema de seguridad estando a miles de kilómetros donde se cometió el delito. (CNS, 2015)

Por lo anterior, la educación no escapa de los continuos avances tecnológicos, y aunque mucho se ha mencionado del divorcio o alejamiento de la educación formal con estos desarrollos, definitivamente la afectan positiva o negativamente. Hoy en día la educación está rodeada de un nuevo lenguaje y de nuevas modas presentes en los hogares, en las calles, en las escuelas etc., en pocas palabras, la forma o manera de educar ha cambiado de un momento histórico a otro.

Hacemos reflexión consiente de la función de la Seguridad Pública y del impacto que tiene en la sociedad mexicana respecto a la carencia de ética, métodos y compromisos en el cumplimiento de su función. Se hace indispensable pensar que la Universidad es una instancia alternativa para que a través de su función y servicio establezca un vínculo de la Seguridad Pública desde nuevos paradigmas de formación disciplinaria en el área específica de este sistema y también inmiscuir a las que no están en relación directa al área.

Partimos de que las funciones sustantivas de la Universidad son la docencia, la investigación, la difusión de la cultura y extensión de los servicios y que se realizarán a través de las entidades académicas, se desprenden las siguientes propuestas como apoyo y promoción a la Ciberseguridad:

- Las Universidades, establezcan convenios con las instancias de seguridad pública, para determinar a través de qué acciones la primera puede promover a la segunda.
- Formar los recursos humanos necesarios para hacer frente a los problemas de seguridad cibernética.
- Elaborar programas estratégicos de comunicación, concientización, capacitación y servicio social a la comunidad universitaria, para inmiscuirla desde su formación a participar en las funciones de Ciberseguridad
- Ubicar a prestadores universitarios de servicio social en actividades de ciberseguridad, de acuerdo a las especialidades disciplinarias del sistema y a aquellas que desempeñen actividades relativas al mismo.
- Las Universidades, de acuerdo al área disciplinaria de la Seguridad Pública, pueden organizar cursos de especialización que sean necesarios de cubrir competentemente en las dependencias de seguridad, así mismo cursos y diplomados, que fomenten en los sujetos una mayor preparación en el áea de ciberseguridad.
- Que la Universidad conciba en su función, no sólo formación disciplinaria del área de especialización, sino que promueva una dimensión integral en la formación de los universitarios, no precisamente en lineamientos establecidos dentro del curriculum formal, sino a través de la promoción de valores respecto a la participación en la seguridad pública, donde intervenga la labor conjunta de la comunidad universitaria (Directivos-Docentes-Estudiantes).

CONCLUSIONES

Cada época ha tenido distintos problemas que resolver, y hoy en día la preocupación de las empresas no es directamente relacionada con la inversión en infraestructura, compra de maquinaria y equipo, de capacitación, manejo de inventarios, entre otros, sino en cómo cuidar la información que se tiene

almacenada en la red, en cómo evitar el robo de identidad y lo más complejo, cómo estar al margen de un desvío de dinero.

Al hablar de Ciberseguridad, casi de inmediato se asocia el concepto de "amenaza". Si hasta hace poco tiempo, la mayor preocupación era proteger algún bien, pero hoy cambia y la prioridad es prevenir los riesgos de ataques cibernéticos.

El ciberespacio tiene una característica jamás nunca vista hasta ahora, que es la exposición. Esa inmensa capacidad de comunicación y de acceso, de intercambio de información con otros individuos y empresa, es un doble problema. Los mismos procesos y las mismas tecnologías pueden dar lugar de igual modo a un nuevo negocio o a una nueva amenaza, alcanzando miles de millones de potenciales clientes o de potenciales víctimas.

Cuando inicio el uso de internet, primero en lo militar y después en la educación, pocas personas aventuraron a pronosticar el gran riesgo que existe por el uso, intercambio, manipulación, compra de información, en realidad no hay privacidad en la red,

La universidad puede y deben jugar un papel importante en la vinculación con la Ciberseguridad, primeramente haciendo conciencia en las personas sobre los riesgos que hay en la red, y después desarrollando conocimiento que permita hacer frente a estas amenazas.

BIBLIOGRAFÍA

Aguayo Quezada, Sergio. *Los usos, abusos y retos de la Seguridad Nacional Mexicana. 1946-1990.* Artículo en el libro *En busca de la seguridad perdida.* Siglo XXI Editores. Primera Edición, 1990. México.

Bunge, M.(2006). La ciencia, su método y su filosofía. México. Nueva Imagen.

Manky Derek (2016). Más ataques y mayor sofisticación, Artículo recuperable en https://colombiadigital.net/actualidad/articulos-informativos/item/9260-mas-ataques-y-mayor-sofisticacion.html.

Minakato Arceo Alberto (2009). "Gestión del conocimiento en educación y transformación de la escuela. Notas para un campo en construcción", en *Sinéctica, revista electrónica de educación*, núm. 32, enero-junio de 2009, ISSN 1665-109X

Molano Adriana (2016). Datos en riesgo: la solución preinstalada en la mitad de los dispositivos del mundo. Archivo recuperable en https://colombiadigital.net/actualidad/articulos-informativos/item/9242-datos-en-riesgo-la-solucion-preinstalada-en-la-mitad-de-los-dispositivos-del-mundo.html

Rodríguez Cafranc Pablo (2016). Ciberseguridad, cómo proteger la información en un mundo digital, Artículo Recuperables en http://blogthinkbig.com/ciberseguridad-como-proteger-la-informacion-en-un-mundo-digital/. Consultado el 20 de octubre de 2016.

Tunnermann Bernheim Carlos (2003). La Universidad Latinoamericana antes los retos del siglo XXI. Colección UDUAL, México.